

ARMY RESEARCH LABORATORY



# A Computing Model for Information Systems Survivability Assessments

by Richard L. zum Brunnen

ARL-TR-1742

August 1998

19980828 029

Approved for public release; distribution is unlimited.

DTIC QUALITY INSPECTED 1

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

# **Army Research Laboratory**

Aberdeen Proving Ground (EA), MD 21010-5423

---

---

**ARL-TR-1742**

**August 1998**

---

## **A Computing Model for Information Systems Survivability Assessments**

**Richard L. zum Brunnen**

Survivability/Lethality Analysis Directorate, ARL

---

## Abstract

---

The Information Systems Survivability Assessment (ISSA) is a process of analytical steps, which the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) applies to networked automated Information Systems (INFOSYS) of military interest.

The goal of SLAD's information systems survivability (ISS) tools, techniques, and methodology (TTM) development program is to generate predictive computer models that predict, as closely as is reasonably possible, the real-world observed behavior of specific information processor properties caused by various real-world stimuli using an agreed-upon set of metrics. These stimuli range from normal network operations to the stressing stimuli caused by various software errors, hardware errors, and the multitude of the different forms of intentional or unintentional misuse and hostile attacks to which an information processor may be subjected.

This report relates the specifics of an analytical model that has been developed for use in ISSAs. This model, the Information Systems Survivability Assessment Model (ISSAM), was designed to be used in modeling the sequence of events and the response of the information systems to different information operations (IO) threats or challenges.

# Table of Contents

|  | <u>Page</u> |
|--|-------------|
| <b>List of Figures</b> .....           | v           |
| <b>List of Tables</b> .....            | v           |
| <b>1. Background</b> .....             | 1           |
| <b>2. Purpose</b> .....                | 2           |
| <b>3. Description</b> .....            | 2           |
| <b>4. Definitions</b> .....            | 4           |
| 4.1 User .....                         | 4           |
| 4.2 Application .....                  | 5           |
| 4.3 Middleware .....                   | 5           |
| 4.4 Operating System .....             | 5           |
| 4.5 Hardware .....                     | 5           |
| 4.6 Networking .....                   | 5           |
| 4.7 Environment .....                  | 6           |
| 4.7.1 <i>Inside Environment</i> .....  | 6           |
| 4.7.2 <i>Outside Environment</i> ..... | 6           |
| <b>5. Discussions</b> .....            | 7           |
| <b>6. Summary</b> .....                | 10          |
| <b>7. Conclusions</b> .....            | 10          |
| <b>8. References</b> .....             | 13          |
| <b>Distribution List</b> .....         | 15          |
| <b>Report Documentation Page</b> ..... | 21          |

INTENTIONALLY LEFT BLANK.

## List of Figures

| <u>Figure</u>                  | <u>Page</u> |
|--------------------------------|-------------|
| 1. Computing Environment ..... | 7           |

## List of Tables

| <u>Table</u>   | <u>Page</u> |
|--|-------------|
| 1. Layers of the ISSAM .....   | 3           |
| 2. Application of the Survivability Model to Potential Compromises ..... | 9           |
| 3. Layers of the ISSAMs .....  | 11          |

INTENTIONALLY LEFT BLANK.



# 1. Background

The Open Systems Interconnection (OSI) reference model is a candidate for an abstract model to guide survivability assessments. The OSI model was developed as the first step toward international standardization of various protocols and is the accepted standard for these developments. The OSI model, as currently configured, is not suited for use as a guide for survivability assessments due to its complexity and variance from real-world configurations. The OSI model breaks the system architecture in multiple layers (seven to be exact), but the model does not specify the exact services and protocols to be found in each layer. It tells what each layer should do. In the computing community, opinions concerning the OSI model vary from individual to individual. For example, according to Garfinkel and Spafford [1]:

*The OSI model is a classic example of what happens when a committee is asked to develop complex specifications without the benefit of first developing working code. On matters such as data transmission, the OSI standards have in general proven to be too cumbersome and complex to fully implement efficiently.*

This model is too abstract for use as a guide for Information Systems Survivability Assessments (ISSA); therefore, another model is needed. For further details on the OSI model, see Tanenbaum [2].

Setting aside its overt complexity raised by Garfinkel and Spafford [1], the OSI architecture could be used for the development of protocols, specific to OSI. This model, therefore, would be best suited for performing survivability assessments on systems using OSI protocols. In this same vain, using the Transmission Control Protocol (TCP)/Internet Protocol (IP) architecture would be best suited for survivability assessments where only TCP/IP protocols are involved. To allow for an unbiased survivability assessment, a model of an information system, independent of any underlying architecture, is required.

## 2. Purpose

In order to perform ISSAs for a multitude of different systems, a model of the information system environment is required to place the analyses into a common framework. The genesis of this report can be found in Table 2.2 on page 28 of Neumann [3]: *“Requirements/Dependence Analysis and Identification of Systemic Inadequacies for Survivable Systems and Networks.”* This work is being performed under SRI Project 1688, Contract DAKF11-97-C0020 for the U.S. Army Research Laboratory (ARL). The scheduled completion date is 25 September 1998. The contract monitor is Mr. Anthony Barnes, ARL, Survivability/Lethality Analysis Directorate (SLAD)/Information Operations (IO) and C4I Branch, <barnesa@doim6.monmouth.army.mil>.

The purpose of this report is to relate the specifics of an analytical model developed for use in ISSA. This model, the Information Systems Survivability Assessment Model (ISSAM), was designed to be used in modeling the sequence of events and the response of the information systems to different IO threats or challenges. This ISSAM is to become a major analytical tool for use in SLAD's ISSAs.

## 3. Description

In the context of an ISSA, an information system is defined by Joint Pub 6-0 [4], as:

*The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.*

This definition covers everything from a single networked computer up to a system of systems, as well as everything in between.

The ISSAM being presented here is broken into eight layers, one more than the OSI model. The layers here are meant to be much less abstract than the OSI layers and can be directly related to real information systems configurations. Table 1 shows the layers of the ISSAM.

**Table 1. Layers of the ISSAM**

|                     |
|---------------------|
| User                |
| Application         |
| Middleware          |
| Operating System    |
| Hardware            |
| Networking          |
| Inside Environment  |
| Outside Environment |

The layers are presented from the perspective of the normal user, that is to say, from the inside out. As one progresses down through the layers in the stack, the complexity of each layer grows with respect to the previous. As the number of components in a layer grows, so does the complexity of the layer. This model could also be depicted as eight concentric circles with the user as the inner-most circle and the outer-most circle being that of the outside environment. Rendered in this way, the complexity of the layers, as well as their scope, can be seen to increase as one progresses out from the center. The area covered by each of the concentric circles can be viewed as being proportional to the complexity of a given layer.

The flexibility, which is gained by the ability to depict this model differently for different situations, is of great benefit to the ISSA process. Depending upon the system being assessed, the analyst has the capability to depict the system in various ways. The number and type of systems that can be assessed is increased. Granularity for each assessment is driven by the requirements of the individual assessment. The picture of the system can be different when the assessment is being done on an individual item or a system of systems. An assessment being done on an individual item (e.g.,

a router, switch, firewall, computer, etc.) begins with a small granularity. When the assessment is being done on a set of networked devices that are in the same room, building, or campus (a local area network), the granularity is greater than that of an individual item. Finally, when the assessment is being done on a system of systems (e.g., a networked collection of local area networks creating a wide area network), the granularity, due to necessity, is much larger than that of a local area network.

Independent of the granularity, if the assessments are done using a framework of the survivability model, presented here, the processes used in the assessments will be identical. Whether one is dealing with a system of systems or an individual item, the operating system interacts with the hardware in the same way. It is also true that the hardware interfaces with the networking elements consistently. These facts lend themselves to the application of a consistent methodology to be used in these assessments. When using this ISSAM, one needs to be mindful of the definitions of the individual layers and apply them consistently when depicting the system. Correct and consistent use of the terminology and definitions across multiple assessments will enable the information produced in one assessment to be directly applicable to other assessments when common elements are found. The definitions of the eight layers are presented in the following section.

## **4. Definitions**

The eight layers are defined as follows:

**4.1 User.** A user is any entity that uses system resources. At any given time, a user can be a person accessing a system through a keyboard at either the desktop workstation or the server consoles. Console access is rare for the average user. Normally, server consoles are secured in a computer room with limited access. At other times, a user may be a process, an agent, a subsystem, or any computer-related entity. The specific identification of an entity is dependent upon the particular event under analysis.

**4.2 Application.** Applications run, or execute, on either servers or desktop workstations. At this level of the ISSAM, the applications have no dependency upon any network resources. These applications depend only upon the local computing platform upon which they are executing.

**4.3 Middleware.** Middleware is a class of application that requires network service to reach full functionality. This is a class of applications, either distributed or network dependent, includes web servers, database management systems, distributed computing, distributed datamining, and data serving to distributed machines, etc.

**4.4 Operating System.** The operating system is the software controlling the hardware of nearly all types of networked devices. This includes servers, desktop workstations, hubs, routers, firewalls, uninterruptable power supplies (UPSs), emergency generators, network switches, etc. The operating system is human intelligible hardware independent computer languages (e.g., C, PASCAL, COBAL, FORTRAN, etc.) compiled (or translated) into hardware dependent machine language. The operating system manages the interfaces between the user, application, and middleware applications and the hardware.

**4.5 Hardware.** The hardware is made up of components, subsystems, and systems. A component is an individual item such as an integrated circuit (IC) chip, cable, disk platter, cooling fan blade, printed circuit board, etc. A subsystem is an assemblage of components or subsystems. For example, a disk drive is a subsystem; it is constructed from motors, read/write heads, disk platters, cables, IC chips, printed circuit cards, etc. To further complicate matters, a disk drive is a component of an input/output (I/O) subsystem. An I/O subsystem is made up of disk drives, printed circuit cards, IC chips, cables, data buses, etc. A system is a collection of subsystems. Examples of subsystems are I/O, graphics, memory, power, etc.

**4.6 Networking.** A network is a collection of devices that communicate. The network is what links the users, applications, middleware applications, operating systems, and hardware together. The devices that create the network are extremely sophisticated, and all run applications, middleware applications, and operating systems to control their hardware. For example, network routers,

switches, and hubs are hardware that is controlled by operating systems running applications to manage middleware applications in order to create a network upon which to pass information. Networking mediums currently include copper, fiber optics, microwave, radio frequencies, satellite communications, etc. Networks, local area and wide area, can be made up of a single, multiple, or all types of mediums. The interfacing of different mediums is handled by switches, routers, hubs, etc.

**4.7 Environment.** The environment can be broken into two pieces: that which can be controlled and that which cannot be controlled. These can also be described as inside (controllable) and outside (uncontrollable).

**4.7.1 Inside Environment.** The inside environment is controllable. For example, the environment in a computer room, an office, a building, or a campus. All types of sites, permanent or temporary, have requirements for power and network connections, both of these come from the outside environment. Permanent (or fixed) sites may have emergency generators as fallbacks in case of loss of power from the outside environment. Temporary (or mobile) sites generally depend upon internal power production, either from batteries or generators. When power production is done within a site, it becomes a part of the inside environment; in this case, the only requirement from the outside environment becomes the network connection. The inside environment may also contain power conditioners; this includes items such as power distribution units, generators, uninterruptable power supplies, surge suppressors, etc. All of these items are controllable even if they rely upon the outside environment for a primary power feed.

**4.7.2 Outside Environment.** The external feeds for network connection and power come from the outside environment to the inside environment. The outside environment is by far the largest piece of the environment. This is the worldly environment, to include terrestrial, marine, aerial, arboreal, spatial, etc. In this environment, events, such as lighting, floods, other weather phenomena, earthquakes, asteroids, meteorites, solar flares, etc., occur. These events, also termed "acts of God," are uncontrollable and in most cases unpredictable.

## 5. Discussions

A generic computing environment is shown in Figure 1. This environment is depicting a generic workplace type of setting and is intended to be a generic client/server configuration, as well as independent environment with desktop machines capable of interacting with a networked compute server. Also note that the environment depicted is independent of the operating systems and specific computing architectures.

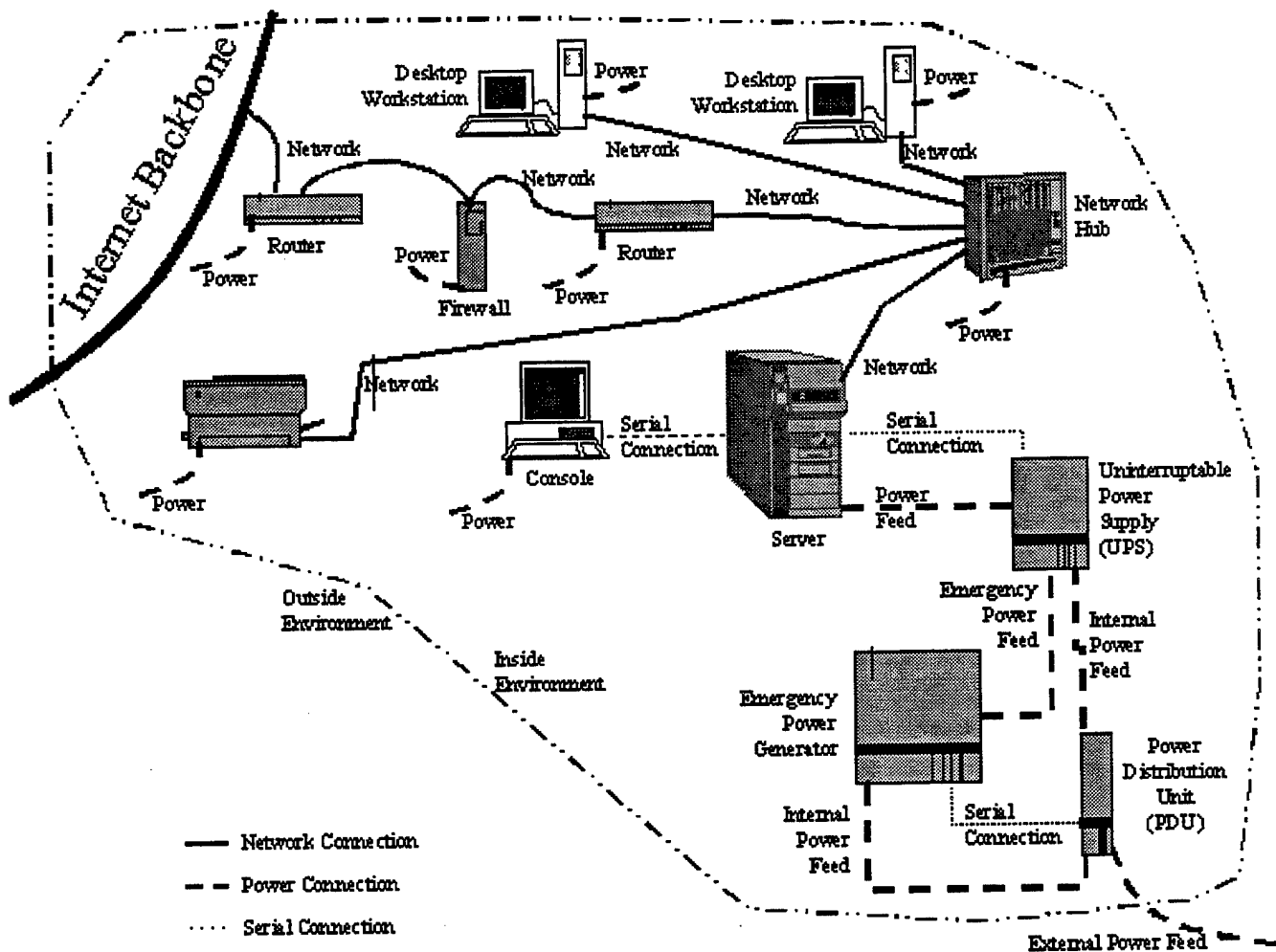


Figure 1. Computing Environment.

Figure 1 is also broken into two environments: the smaller, controllable, inside environment and the much larger, uncontrollable, outside environment. Feeds for both the network connection and power feed are shown crossing from one environment into the other. The network connection could be either a physical connection made with some type of cable or an ether type of connection using radio or microwave frequencies. The network example shown in Figure 1 is totally fictitious and was created solely for illustrative purposes.

Each of the devices shown in Figure 1 can be represented using the layers from Table 1. The different types of devices are represented differently. For example, the desktop workstations are represented by the user through the inside environment layers, with dependencies on the outside environment (as do all networked devices). In contrast to the desktop workstation, the emergency power generator, which also has dependencies upon the outside environment, can be represented with a much smaller number of layers. These consist of the application (waiting for a signal through the serial connection), the operating system (which manages all the hardware), the hardware, and the inside environment layers. It can also be seen that different stimuli are represented by different types of interactions of the model layers. One place where these interactions are detailed is in the item requirements and specifications packages.

Table 2 reproduces Table 2.2 from Neumann [3]. This table shows how the level of abstraction used in the model can also be used to describe possible compromise. Garfinkel and Spafford [1] also present a detailed discussion of this table.

With the structure as presented in Table 2, compromise can come from three sources: outside, within, or below. Within an information systems survivability framework, compromise is used as a very broad term meaning that an IO on information warfare (IW) event has been successful. Neumann characterizes compromise from the three sources as follows:

- Compromise from outside typically originates from an access point that is nominally external to the component being compromised.



**Table 2. Application of the Survivability Model to Potential Compromises**

| Layer of Abstraction | Compromise From Outside   | Compromise From Inside  | Compromise From Below  |
|----------------------|---|---|--|
| Outside Environment  | —   | Acts of God, earthquakes, lighting, etc.  | Chernobyl-like disasters caused by users or operators  |
| User                 | Masqueraders  | Accidental mistakes<br>Intentional misuse   | Application system outage or service denial  |
| Application          | Penetration of application integrity  | Programming errors in application code  | Application (e.g., DBMS) undermined within operating systems (OSs)                               |
| Middleware           | Penetration of Web and Database Management System (DBMS) servers                              | Trojan horsing of Web and DBMS servers  | Subversion of middleware from OS or network operations   |
| Networking           | Penetration of routers, firewalls; denials of service   | Trojan horsing of network software  | Capture of crypto keys within OS<br>Exploitation of lower protocol layers                        |
| Operating System     | Penetration of OS by unauthorized users   | Flawed OS software<br>Trojan-horsed OS<br>Tampering by privileged processes                                       | OS undermined from within hardware; faults exceeding fault tolerance; hardware flaws or sabotage |
| Hardware             | Externally generated electromagnetic or other interference<br>External power utility glitches | Bad hardware design and implementation<br>Hardware Trojan horses<br>Unrecoverable faults<br>Internal interference | Internal power irregularities  |
| Inside Environment   | Malicious or accidental acts  | Internal power supplies, tripped breakers, UPS/battery failures   | —  |

- Compromise from within typically originates inside a particular component that is compromised, existing at a given level of abstraction.
- Compromise from below is initiated at a lower layer of abstraction than the layer at which compromise of a given component occurs.

Given the data from Table 2 and the characterization of these sources of compromise, it becomes clear that a system may be inherently compromisable in a variety of ways. The goals of the ISSA process are to determine the ways in which a system is compromisable, determine the likelihood of occurrence and the resulting impact on the system due to these compromises, and recommend ways to avoid these compromises. A systematic, consistent, and correct use of the model presented here, as well as a common methodology used in the ISSAs, will enable comprehensive and robust assessments to be performed.

## **6. Summary**

The abstract computing model described here, shown in Table 3, is not tied to any particular protocol family or to any one system architecture. This model is structured robustly enough that multiple machine architectures, as well as different protocol families, can be modeled. The model is constructed of eight separate layers. When an event is modeled, the appropriate layers are traversed vertically both into and out of systems as required. Events are modeled by the interaction of the layers. This model is well suited to vulnerability assessments.

## **7. Conclusions**

A model of a real-world computing environment has been developed. This model is designed for use in ISSAs. This model is of hierarchical construction consisting of eight layers. These layers progress from the user through layers associated with computing machinery and networks and finally

**Table 3. Layers of the ISSAMs**

|                     |
|---------------------|
| User                |
| Application         |
| Middleware          |
| Operating System    |
| Hardware            |
| Networking          |
| Inside Environment  |
| Outside Environment |

to the environment. This model can be used to depict machines of different architectures and multiple networks performing a variety of functions. The model is suitable for use on both local area networks as well as wide area networks and is capable of incorporating both controllable and uncontrollable environmental concerns. The flexibility intrinsic to this model makes it comprehensive enough to model permanent (or fixed) installations, transitory (or temporary), as well as mobile (or dynamic), configurations. In military parlance, this model is capable of modeling the global information infrastructure, the military information infrastructure, the sustaining base, camps, posts, stations, and tactical maneuvering units. These can be modeled independently or in any combination, to any desired level of detail (granularity) required for the particular assessment.

The consistent use of this model across ISSAs will allow for tremendous amounts of leveraging of information across multiple assessments of different weapons platforms and military systems. The use of a single model will add consistency to the analysis process.

INTENTIONALLY LEFT BLANK.

## 8. References

1. Garfinkel, S., and G. Spafford. *Practical UNIX and Internet Security*. Second Edition, Sebastopol, CA: O'Reilly and Associates, Inc., 1996.
2. Tanenbaum, A. S. *Computer Networks*. Second Edition, Englewood Cliffs, NJ: Prentice-Hall, Inc., 1989.
3. Neumann, P. G. "Requirements/Dependence Analysis and Identification of Systemic Inadequacies for Survivable Systems and Networks." Computer Science Laboratory, SRI International, Draft, DAKF11-97-C0020, Survivability/Lethality Analysis Directorate, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, 30 January 1998.
4. Joint Pub 6-0. "Doctrine for Command, Control, Communications, and Computers (C<sup>4</sup>) Systems Support to Joint Operations." 3 June 1992.
5. Stallings, W. *Handbook of Computer-Communications Standards, Volume 1, The Open Systems Interconnection (OSI) Model and OSI-Related Standards*. Indianapolis, IN: Howard W. Sams and Company, 1987.
6. Stallings, W. *Data and Computer Communications*. Second Edition, New York, NY: Macmillan Publishing Company, 1988.
7. Black, U. *TCP/IP and Related Protocols*. New York, NY: McGraw-Hill, Inc., 1992.
8. Feit, S. *TCP/IP - Architecture, Protocols, and Implementation*. New York, NY: McGraw-Hill, Inc., 1993.

INTENTIONALLY LEFT BLANK.

| NO. OF<br>COPIES | ORGANIZATION   |
|------------------|--|
| 2                | DEFENSE TECHNICAL<br>INFORMATION CENTER<br>DTIC DDA<br>8725 JOHN J KINGMAN RD<br>STE 0944<br>FT BELVOIR VA 22060-6218  |
| 1                | HQDA<br>DAMO FDQ<br>DENNIS SCHMIDT<br>400 ARMY PENTAGON<br>WASHINGTON DC 20310-0460                                    |
| 1                | DPTY ASSIST SCY FOR R&T<br>SARD TT F MILTON<br>RM 3EA79 THE PENTAGON<br>WASHINGTON DC 20310-0103                       |
| 1                | OSD<br>OUSD(A&T)/ODDDR&E(R)<br>J LUPO<br>THE PENTAGON<br>WASHINGTON DC 20301-7100                                      |
| 1                | CECOM<br>SP & TRRSTRL COMMCTN DIV<br>AMSEL RD ST MC M<br>H SOICHER<br>FT MONMOUTH NJ 07703-5203                        |
| 1                | PRIN DPTY FOR TCHNLGY HQ<br>US ARMY MATCOM<br>AMCDCG T<br>M FISETTE<br>5001 EISENHOWER AVE<br>ALEXANDRIA VA 22333-0001 |
| 1                | DPTY CG FOR RDE HQ<br>US ARMY MATCOM<br>AMCRD<br>BG BEAUCHAMP<br>5001 EISENHOWER AVE<br>ALEXANDRIA VA 22333-0001       |
| 1                | INST FOR ADVNCD TCHNLGY<br>THE UNIV OF TEXAS AT AUSTIN<br>PO BOX 202797<br>AUSTIN TX 78720-2797                        |

| NO. OF<br>COPIES | ORGANIZATION  |
|------------------|---|
| 1                | GPS JOINT PROG OFC DIR<br>COL J CLAY<br>2435 VELA WAY STE 1613<br>LOS ANGELES AFB CA 90245-5500   |
| 3                | DARPA<br>L STOTTS<br>J PENNELLA<br>B KASPAR<br>3701 N FAIRFAX DR<br>ARLINGTON VA 22203-1714   |
| 1                | US MILITARY ACADEMY<br>MATH SCI CTR OF EXCELLENCE<br>DEPT OF MATHEMATICAL SCI<br>MDN A MAJ DON ENGEN<br>THAYER HALL<br>WEST POINT NY 10996-1786 |
| 1                | DIRECTOR<br>US ARMY RESEARCH LAB<br>AMSRL CS AL TP<br>2800 POWDER MILL RD<br>ADELPHI MD 20783-1145  |
| 1                | DIRECTOR<br>US ARMY RESEARCH LAB<br>AMSRL CS AL TA<br>2800 POWDER MILL RD<br>ADELPHI MD 20783-1145  |
| 3                | DIRECTOR<br>US ARMY RESEARCH LAB<br>AMSRL CI LL<br>2800 POWDER MILL RD<br>ADELPHI MD 20783-1145   |
|                  | <u>ABERDEEN PROVING GROUND</u>  |
| 4                | DIR USARL<br>AMSRL CI LP (305)  |

| <u>NO. OF<br/>COPIES</u> | <u>ORGANIZATION</u>  |
|--------------------------|--|
| 1                        | <p>OUSD AT STRT TAC SYS<br/> DR SCHNEITER<br/> RM 3E130<br/> 3090 DEFENSE PENTAGON<br/> WASHINGTON DC 20310-3090</p>                     |
| 1                        | <p>OASD C31<br/> DR SOOS RM 3E194<br/> 6000 DEFENSE PENTAGON<br/> WASHINGTON DC 20301-6000</p>   |
| 1                        | <p>UNDER SEC OF THE ARMY<br/> DUSA OR<br/> ROOM 2E660<br/> 102 ARMY PENTAGON<br/> WASHINGTON DC 20310-0102</p>                           |
| 1                        | <p>ASST SECY ARMY RESEARCH<br/> DEVELOPMENT ACQUISITION<br/> SARD ZD ROOM 2E673<br/> 103 ARMY PENTAGON<br/> WASHINGTON DC 20310-0103</p> |
| 1                        | <p>ASST SECY ARMY RESEARCH<br/> DEVELOPMENT ACQUISITION<br/> SARD ZP ROOM 2E661<br/> 103 ARMY PENTAGON<br/> WASHINGTON DC 20310-0103</p> |
| 1                        | <p>ASST SECY ARMY RESEARCH<br/> DEVELOPMENT ACQUISITION<br/> SARD ZS ROOM 3E448<br/> 103 ARMY PENTAGON<br/> WASHINGTON DC 20310-0103</p> |
| 1                        | <p>OADCSOPS FORCE DEV DIR<br/> DAMO FDZ<br/> ROOM 3A522<br/> 460 ARMY PENTAGON<br/> WASHINGTON DC 20310-0460</p>                         |
| 1                        | <p>OADCSOPS FORCE DEV DIR<br/> DAMO FDW<br/> RM 3C630<br/> 460 ARMY PENTAGON<br/> WASHINGTON DC 20310-0460</p>                           |

| <u>NO. OF<br/>COPIES</u> | <u>ORGANIZATION</u>   |
|--------------------------|---|
| 1                        | <p>HQ USAMC<br/> DEP CHF OF STAFF FOR RDA<br/> AMCRD<br/> 5001 EISENHOWER AVE<br/> ALEXANDRIA VA 22333-0001</p>   |
| 1                        | <p>ARMY TRNG &amp; DOCTRINE COM<br/> ATCD B<br/> FT MONROE VA 23561-5000</p>                                      |
| 1                        | <p>ARMY TRADOC ANL CTR<br/> ATRC W<br/> MR KEINTZ<br/> WSMR NM 88002-5502</p>                                     |
| 1                        | <p>ARMY RESEARCH LABORATORY<br/> AMSRL SL<br/> PLANS AND PGMS MGR<br/> WSMR NM 88002-5513</p>                     |
| 1                        | <p>ARMY RESEARCH LABORATORY<br/> AMSRL SL E<br/> MR SHELBURNE<br/> WSMR NM 88002-5513</p>                         |
| 1                        | <p>ARMY RESEARCH LABORATORY<br/> AMSRL ST<br/> DR ROCCHIO<br/> 2800 POWDER MILL RD<br/> ADELPHI MD 20783-1197</p> |



NO. OF  
COPIES ORGANIZATION

ABERDEEN PROVING GROUND

- |   |  |
|---|--|
| 1 | ARMY TEST EVAL COM<br>AMSTE TA<br>APG MD 21005-5055  |
| 1 | US ARMY EVAL ANALYSIS CTR<br>CSTE EAC MR HUGHES<br>4120 SUSQUEHANNA AVE<br>APG MD 21005-3013     |
| 1 | US ARMY EVAL ANALYSIS CTR<br>CSTE EAC SV DR HASKELL<br>4120 SUSQUEHANNA AVE<br>APG MD 21005-3013 |
| 1 | ARMY RESEARCH LABORATORY<br>AMSRL SL<br>DR WADE<br>APG MD 21005-5068                             |
| 2 | ARMY RESEARCH LABORATORY<br>AMSRL SL B<br>MS SMITH<br>W WINNER<br>APG MD 21005-5068              |
| 1 | ARMY RESEARCH LABORATORY<br>AMSRL SL E<br>DR STARKS<br>APG EA MD 21010-5423                      |

NO. OF  
COPIES   ORGANIZATION

4      USARL  
         AMSRL SL EI  
         MR NOWAK  
         MR MEINCKE  
         MR BARNES  
         MR LURSKI  
         FORT MONMOUTH NJ  
         07703-5602

2      USARL  
         AMSRL SL EM  
         MR PALOMO  
         MR OCHOA  
         WSMR NM 88002-5513

8      USARL  
         AMSRL SL EI  
         CPT(P) THEODOSS  
         MS CHRISTIANSON  
         MR MAREZ  
         MR WILLIAMS  
         MR MCDONALD  
         MS JIMENEZ  
         MR SWEARINGEN  
         SGT GOWINS  
         WSMR NM 88002-5513

2      USARL  
         AMSRL SL ET  
         MS THOMPSON  
         DR YEE  
         WSMR NM 88002-5513

3      USARL  
         AMSRL SL EA  
         MR FLORES  
         MR LANDIN  
         MR STAY  
         WSMR NM 88002-5513

3      USARL  
         AMSRL SL EV  
         DR MORRISON  
         MR LUJAN  
         MR SPEZIALE  
         WSMR NM 88002-5513

NO. OF  
COPIES   ORGANIZATION

2      USARL  
         AMSRL IS  
         DR GANTT  
         LTC WALCZAK  
         2800 POWDER MILL RD  
         ADELPHI MD 20783-1197

1      COMMANDER NGIC  
         AING SBE  
         MR TERRY  
         220 SEVENTH ST NE  
         CHARLOTTESVILLE VA  
         22902-5396

1      COMMANDER INSCOM  
         LIWA  
         MS MEHAN  
         8825 BEULAH ST  
         FORT BELVOIR VA 22060-5246

1      LTC B MALONEY  
         235 B BARNARD LOOP  
         WEST POINT NY 10996

ABERDEEN PROVING GROUND

40     DIR USARL  
         AMSRL SL EI  
         MR PANUSKA  
         MR ZUM BRUNNEN (25 CPS)  
         AMSRL SL B  
         MR SANDMEYER  
         AMSRL SL EM  
         DR FEENEY  
         AMSRL SL ET  
         MR BAYLOR  
         AMSRL SL BG  
         MS YOUNG  
         MR FRANZ  
         MR KUSS  
         DR LIU  
         MR PLOSKONKA  
         MR ZIGLER  
         AMSRL SL BA  
         MS RITONDO  
         MR VOGEL  
         AMSRL SL BE  
         MR BELY  
         MR PETTY

| <u>NO. OF<br/>COPIES</u> | <u>ORGANIZATION</u>            |
|--------------------------|--------------------------------|
|                          | AMSRL SL BN<br>MR FARENWALD    |
| 1                        | USAEAC<br>CSTE EAC SV MR MYERS |

INTENTIONALLY LEFT BLANK.

| REPORT DOCUMENTATION PAGE  |   |  | Form Approved<br>OMB No. 0704-0188   |  |
|--|---|--|--------------------------------------|--|
| <small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project(0704-0188), Washington, DC 20503.</small>   |   |  |                                      |  |
| 1. AGENCY USE ONLY (Leave blank)   | 2. REPORT DATE<br>August 1998                               | 3. REPORT TYPE AND DATES COVERED<br>Final, Jan - Mar 98        |                                      |  |
| 4. TITLE AND SUBTITLE<br><br>A Computing Model for Information Systems Survivability Assessments   |   | 5. FUNDING NUMBERS<br><br>8LEH40                               |                                      |  |
| 6. AUTHOR(S)<br><br>Richard L. zum Brunnen   |   |  |                                      |  |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br><br>U.S. Army Research Laboratory<br>ATTN: AMSRL-SL-EI<br>Aberdeen Proving Groun (EA), MD 21010-5423   |   | 8. PERFORMING ORGANIZATION<br>REPORT NUMBER<br><br>ARL-TR-1742 |                                      |  |
| 9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)   |   | 10. SPONSORING/MONITORING<br>AGENCY REPORT NUMBER              |                                      |  |
| 11. SUPPLEMENTARY NOTES  |   |  |                                      |  |
| 12a. DISTRIBUTION/AVAILABILITY STATEMENT<br><br>Approved for public release; distribution is unlimited.  |   |  | 12b. DISTRIBUTION CODE               |  |
| 13. ABSTRACT (Maximum 200 words)<br><p>The Information Systems Survivability Assessment (ISSA) is a process of analytical steps, which the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) applies to networked automated Information Systems (INFOSYS) of military interest.</p> <p>The goal of SLAD's information systems survivability (ISS) tools, techniques, and methodology (TTM) development program is to generate predictive computer models that predict, as closely as is reasonably possible, the real-world observed behavior of specific information processor properties caused by various real-world stimuli using an agreed-upon set of metrics. These stimuli range from normal network operations to the stressing stimuli caused by various software errors, hardware errors, and the multitude of the different forms of intentional or unintentional misuse and hostile attacks to which an information processor may be subjected.</p> <p>This report relates the specifics of an analytical model that has been developed for use in ISSAs. This model, the Information Systems Survivability Assessment Model (ISSAM), was designed to be used in modeling the sequence of events and the response of the information systems to different information operations (IO) threats or challenges.</p> |   |  |                                      |  |
| 14. SUBJECT TERMS<br>information systems, information operations, information warfare, survivability, assessment, modeling   |   |  | 15. NUMBER OF PAGES<br>22            |  |
|  |   |  | 16. PRICE CODE                       |  |
| 17. SECURITY CLASSIFICATION<br>OF REPORT<br>UNCLASSIFIED   | 18. SECURITY CLASSIFICATION<br>OF THIS PAGE<br>UNCLASSIFIED | 19. SECURITY CLASSIFICATION<br>OF ABSTRACT<br>UNCLASSIFIED     | 20. LIMITATION OF ABSTRACT<br><br>UL |  |

INTENTIONALLY LEFT BLANK.

## USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-TR-1742 (zum Brunnen) Date of Report August 1998

2. Date Report Received \_\_\_\_\_

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

CURRENT  
ADDRESS

\_\_\_\_\_  
Organization

\_\_\_\_\_  
Name

\_\_\_\_\_  
E-mail Name

\_\_\_\_\_  
Street or P.O. Box No.

\_\_\_\_\_  
City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD  
ADDRESS

\_\_\_\_\_  
Organization

\_\_\_\_\_  
Name

\_\_\_\_\_  
Street or P.O. Box No.

\_\_\_\_\_  
City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)  
(DO NOT STAPLE)